TAB: B
TOPIC: OPSEC Policy
CHANGE: N/A

APPENDIX: 6
DATE ORIGINAL PUBLISHED: 10 SEP 06
DATE LATEST CHANGE PUBLISHED: N/A

DRAFT

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Fires Brigade, 4ID – Operations Security (OPSEC) Program

1. (U) References.

a. (U) National Security Decision Directive (NSDD) No. 298, National Operations Security Program, January 22, 1988.

b. (U) DoD Directive 5205.2, DoD Operations Security (OPSEC) Program.

c. (U) Interagency OPSEC Support Staff (IOSS), Glossary of OPSEC Terms, Rev 1998.

d. (U) DoD Directive 5200.39, Security, Intelligence, and Counterintelligence Support to Acquisition Programs (10 Sep 97).

e. (U) SECDEF Message DTG 141553Z JAN 03.

f. (U) JP 3-13 Joint Doctrine for Information Operations.

g. (U) CJCSI 3213.01A, Joint Operations Security.

h. (U) DEPSECDEF Memo, Operations Security, Jun 2003.

i. (U) JP 3-54, Joint Doctrine for Operations Security.

2. (U) Purpose. This Directive establishes the Fires Brigade Operations Security (OPSEC) program and provides policy, assigns responsibilities and implements above references.

3. (U) General.

a. (FOUO) The objective of OPSEC is to preserve the effectiveness of military capabilities and maintain the elements of initiative, surprise, and security. The purpose of this SOP is to provide guidance to Fires Brigade personnel for the implementation of OPSEC within the Fires Brigade during operations.

b. (FOUO) Essential secrecy depends on traditional security programs to deny classified information and OPSEC to identify, control, and limit vulnerabilities and indicators. OPSEC must be incorporated during the planning, preparation, execution, and post-execution of operations and activities.

c. (FOUO) Adversaries depend primarily on detectable activities and open sources for information about Fires Brigade intentions and capabilities. Operations (e.g., training, test, exercise, and development) involve many detectable activities and significant amounts of open source information. As world conditions change, today's ally may be tomorrow's adversary or competitor.

4. (U) Applicability.

a. (U) This Directive applies to all Fires Brigade Subordinate Commanders, Units, and Staff.

b. (U) The OPSEC program shall be applied to DA civilians since they must provide adequate protection of critical or sensitive information, activities or operations of the command, its elements and/or directly or indirectly associated with a specific contract.

5. (U) Definitions.

a. (U) Operations Security (OPSEC). OPSEC is a process of identifying Critical Information (CI) and subsequently, analyzing friendly actions attendant to military operations and other activities to:

b. (FOUO) Identify those actions that can be observed by adversaries.

c. (FOUO) Determine indicators that could be interpreted or pieced together to derive critical information.

d. (FOUO) Identify friendly vulnerabilities and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

e. (U) OPSEC is distinct from Information Security (INFOSEC), Communications Security (COMSEC), and Physical Security.

f. (FOUO) Critical Information (CI) is information that must be protected. It must keep an adversary from gaining a significant operational, economic, political, or technological advantage and prevent adverse impact on friendly mission accomplishment.

g. (FOUO) OPSEC Countermeasures (CM) are those measures taken by friendly forces to make an adversary change his method of collecting CI, observing friendly actions, or conducting operations. CMs are designed to cause the adversary to change his behavior, making him become more overt and thus making him more susceptible to detection by friendly forces.

6. (U) Policy.

a. (U) In accordance with Reference 1a and 1b, MNF-I and subordinate commanders will establish a formal OPSEC program that:

(1) (FOUO) Assigns responsibility for OPSEC direction and implementation.

(2) (FOUO) Requires a plan to implement the OPSEC program.

(3) (FOUO) Trains all personnel, commensurate with their positions and security clearances on hostile intelligence threats and the OPSEC process.

b. (FOUO) OPSEC is a leadership responsibility. Leaders at all levels are responsible for maintaining their organization’s OPSEC program and accepting the risk of not incorporating countermeasures (CM).

7. (U) Responsibilities.

a. (U) Battalion and Battery/ Company Commanders.

(1) (FOUO) Maintain written OPSEC programs at battalion and higher echelons.

(2) (FOUO) Maintain a copy of the Fires Brigade OPSEC Policy on file at battalion HQs.

(3) (FOUO) Appoint an OPSEC Officer in writing.

(4) (FOUO) Commanders implement this OPSEC SOP throughout their battalions.

(5) (FOUO) Commanders integrate OPSEC into all activities to provide maximum protection of all functions and activities and preserve essential secrecy.

(6) (FOUO) Ensure OPSEC training is conducted in accordance with references and/or approved Regulations, Pamphlets, and Doctrine.

(7) (FOUO) Approve the organization's CI list and circulate to all members of the command.

(8) (FOUO) Conduct OPSEC awareness training for all personnel.

(9) (FOUO) Assign a unit OPSEC Officer in writing and provide a copy of appointment orders to the Fires Brigade S-2 Shop.

a. (FOUO) The OPSEC Officer should be an operations staff officer or Battery/ Company XO or noncommissioned officer (NCO), in the grade of E7 or above and have a minimum of 3-6 months time remaining on station.

b. (FOUO) The OPSEC Officer responsibilities will include specific requirements in accordance with references.

Formatted: Bullets and Numbering

c. (FOUO) All OPSEC Officers will attend OPSE 2400 course.

b. (FOUO) Unit OPSEC points of contact will report to the Fires Brigade OPSEC Officer in the following format:

(1) (FOUO) Overview of OPSEC program status-quarterly.

Formatted: Bullets and Numbering

(2) (FOUO) Training / indoctrination program activities-quarterly.

Formatted: Bullets and Numbering

(3) (FOUO) Forecast of OPSEC activities for next reporting period.

Formatted: Bullets and Numbering

(4) (FOUO) Lessons learned- semi annually.

(5) (FOUO) Problems and recommendations as they occur.

c. (U) Fires Brigade OPSEC Officer.

(1) (FOUO) Prepare and recommend changes to Fires Brigade policies based on guidance from the command group.

(2) (FOUO) Prepare, recommend, and supervise execution of the Fires Brigade OPSEC Program.

(3) (FOUO) Assist S3 in development of countermeasures.

(4) (FOUO) Ensure that OPSEC training (initial, refresher, and recurring) is conducted in accordance with references and/or approved Regulations, Pamphlets, and Doctrine.

(5) (FOUO) Coordinate with Force Protection and G2 to ensure an OPSEC review is conducted prior to the release of information concerning the command, command programs, projects, activities, and operations.

(6) (FOUO) Ensure OPSEC awareness briefings to assigned personnel are conducted with the Newcomer's Brief.

(7) (FOUO) Develop and disseminate OPSEC awareness related material to subordinate units.

(8) (FOUO) Assist subordinate unit OPSEC Coordinators when required.

(9) (FOUO) As requested, assist other staff elements with development of their OPSEC CMs, plans, and training programs.

d. (U) Public Affairs Officer.

(1) (FOUO) Do not divulge CI in the public release of information. Ensure releases do not provide enough data for adversaries to target friendly personnel's families back in the U.S. or other bases and stations.

(2) (FOUO) Follow the Generic CM List enclosed in the Fires Brigade OPSEC Policy.

e. (U) All Fires Brigade Staff Elements.

(1) (FOUO) Comply with established OPSEC SOPs and security practices for the protection / control of CI.

(2) (FOUO) Maintain awareness of changing adversary intelligence collection threats.

(3) (FOUO) Handle any attempt by unauthorized personnel to solicit sensitive or critical information as a Subversion And Espionage Directed against the Army (SAEDA) incident per AR 381-2. This regulation requires personnel to *not* report any SAEDA incidents to the chain of command and *only* report SAEDA incidents to the local counter intelligence detachment.

(4) (FOUO) Follow the generic CM List that is enclosed in the Fires Brigade OPSEC policy.

c. (FOUO) S-6. Identify critical information systems, nodes, networks, cell phones, Iridium, and Thuraya that require protection. Also, ensure the communications security program supports the OPSEC plan.

d. (U) The Fires Brigade Program Manager shall:

(1) (FOUO) Develop OPSEC policy, guidance, and instructions.

(2) (FOUO) Advise the Commander, Fires Brigade of the status of the OPSEC Program, to include plans, developments, innovations, problems, and solutions.

(3) (FOUO) Develop and maintain an OPSEC plan that includes, at a minimum, generic CM applicable to all friendly personnel and publishing a CI list.

8. (U) Collection Threat.

a. (FOUO) OPSEC protects CI. While it is possible that almost any adversary eventually may uncover sensitive or classified information, OPSEC CM hinders intelligence gathering and makes it more difficult, time consuming, and expends their resources, capabilities, and financing.

b. (FOUO) The following OPSEC threat assumptions are made:

(1) (FOUO) Anti-coalition elements are collecting information of intelligence value to assist them in continued attacks against Coalition Forces.

(2) (FOUO) Anti-coalition elements will collect intelligence or valued information by any method available.

(3) (FOUO) Anti-coalition elements will attempt to collect unclassified as well as classified information.

(4) (FOUO) Adversaries are at least as intelligent as friendly forces.

(5) (FOUO) All non-secure communications are being monitored and analyzed for CI.

(6) (FOUO) All paper documents, to include envelope addresses, post-it notes, emails, and forms that are placed in the trash, are being collected and read.

c. (FOUO) Fires Brigade threat forces are Former Regime Elements (FRE), Foreign Intelligence Services (FIS), and extremists, to include foreign terrorists and start-up militias, criminals, computer system penetrators (hackers), and insiders. OPSEC must consider not only the actual threat of adversaries who obtain information to harm Coalition Forces, but also consider other groups or individuals who collect information that would then be available to adversaries.

d. (FOUO) Signal Intelligence (SIGINT). FRE and FIS have access to portable commercially available intercept equipment, which is limited to voice intercept of non-encrypted non-frequency hopping emitters. The use of hand-held push to talk radios, such as Motorola's, cellular phones, Thuraya / Iridium, and any non-secure communication should be highly discouraged. Another aspect of SIGINT is Computer Security (COMPUSEC). Diligence in obeying security regulations can prevent the loss of secure information. Sending CI, regardless of classification, via secure e-mail is a key to security.

e. (FOUO) HUMINT. HUMINT is the primary method used by our adversaries. The type of collection depends on the purpose and target. Be aware of surveillance targeting, ambushes, kidnappings, or assassinations, as well as solicitation of operational information and tactics, techniques, and procedures (TTPs) for use in planning countermeasures. Friendly personnel are targeted for sale and solicitation of information. Careless discussions on how to conduct or plan attacks can lead to the enemy developing countermeasures. Simple conversations (even when dining) reveal a great deal about military operations. HUMINT sources may be imbedded into Non Government Organizations (NGOs) and contract organizations. An agent operating in close proximity to coalition forces can gather a great deal of information. Information such as types of equipment, number of vehicles, which directions a convoy is going can be converted into actionable intelligence.

f. (FOUO) IMINT. IMINT collection involves a broad spectrum of imaging techniques ranging from highly sophisticated satellite systems to hand-held camera phones. The imagery threat is of increasing concern because of the availability of high-quality pictures. Not only do foreign governments and intelligence services use the capabilities of satellite imagery, several sell it commercially. The most common form of IMINT used by anti-coalition forces is photography or video surveillance. Photography is used in planning attacks on fixed sites. The use of camouflage netting and deceptive lighting prevents accurate targeting and the mapping of facilities.

g. (FOUO) Open Source Intelligence (OSINT). Open Source information or OSINT is information readily available in non-secure emails / phone calls, news services or publicly distributed reports. It provides a very accurate picture of operations and is widely used by the enemy. OSINT is the best indicator of TTPs; care must be taken in what is said to the media and what information is given to the local populace. Screening of publicly available or open source material is often an early phase of an intelligence collection operation.

9. (U) OPSEC Process. The OPSEC process applies to all phases of an activity, function, or operation and is used in OPSEC planning. The five steps are:

a. (FOUO) Identification of Critical Information (CI). The purpose of this step is to determine what needs protection. Critical information consists of specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishments. CI also consists of OPSEC indicators, which are friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive CI. Identify key questions that adversary officials and intelligence systems are likely to ask about friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. These questions are the Essential Elements of Friendly Information (EEFI). Answers to EEFI are critical information (CI). The answers to the questions are the items that must be protected.

(1) (FOUO) What specific unclassified, but sensitive, facts about friendly activities would an adversary need to disrupt operations or endanger friendly forces?

(2) (FOUO) What critical information does the adversary already know?

(3) (FOUO) What OPSEC indicators will friendly activities create about critical information not already known by the adversary?

(4) (FOUO) What indicators can the adversary actually collect? This depends on the capabilities of the adversary's intelligence systems.

(5) (FOUO) What indicators will the adversary be able to use to the disadvantage of friendly forces? The answers to this last question are the OPSEC vulnerabilities.

b. (FOUO) Analysis of Threat. This action involves the research and analysis of intelligence information, counterintelligence, reports, and open source information to identify who the likely adversaries are to the planned operation. Consider the following questions:

(1) Who is the adversary? (Who has the intent and capability to take action against a planned operation?)

(2) What are the adversary's goals? (What does the adversary want to accomplish?)

(3) What is the adversary's strategy for opposing the planned operation? (What actions might the adversary take?)

(4) What critical information does the adversary already know about the operation? (What information is it too late to protect?)

(5) What are the adversary's intelligence collection capabilities?

c. (FOUO) Analysis of Vulnerabilities. The purpose of this action is to identify an operation's or activity's OPSEC vulnerabilities. It requires examining each aspect of the planned operation to identify any OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. Vulnerability exists when the adversary is capable of collecting an OPSEC indicator or CI, correctly analyzing it, and then taking timely action.

(1) (FOUO) What indicators (friendly actions and open source information) of critical information not known to the adversary will be created by the friendly activities that will result from the planned operation?

(2) (FOUO) What indicators can the adversary actually collect?

(3) (FOUO) What indicators will the adversary be able to use to the disadvantage of friendly forces? (Can the adversary analyze the information, make a decision, and take appropriate action in time to interfere with the planned operation?)

d. (FOUO) Assessment of Risk. This action has two components. First, planners analyze the OPSEC vulnerabilities identified in the previous action and identify possible OPSEC countermeasures for each vulnerability. Second, specific OPSEC countermeasures are selected for execution based upon a risk assessment done by the commander and staff.

(1) (FOUO) OPSEC countermeasures reduce the probability of the adversary either collecting the indicators or being able to correctly analyze their meaning.

(2) (FOUO) OPSEC measures can be used to: (1) Prevent the adversary from detecting an indicator; (2) Provide an alternative analysis of an indicator; and/or (3) Attack the adversary's collection system.

(3) (FOUO) OPSEC measures include, among other actions, cover, concealment, camouflage, deception, intentional deviations from normal patterns, and direct strikes against the adversary's intelligence system.

(4) (FOUO) More than one possible countermeasure may be identified for each vulnerability. Conversely, a single countermeasure may be used for more than one vulnerability.

(5) (FOUO) OPSEC measures usually entail some cost in time, resources, personnel, or interference with normal operations. If the cost to mission effectiveness exceeds the harm that an

adversary could inflict, then the application of the measure is inappropriate. Because the decision not to implement a particular OPSEC measure entails risks, this step requires command involvement.

e. (FOUO) Application of appropriate OPSEC Countermeasures. The purpose of this step is to apply OPSEC Countermeasures, chosen by the commander, to current operations as well as planning and preparation for future operations. The implementation of the specific OPSEC measure will be addressed in the OPSEC Annex of each operations order (OPORD). During the execution of OPSEC countermeasures, the reaction of adversaries to the countermeasures is monitored to determine their effectiveness and to provide feedback. Planners use that feedback to adjust ongoing activities and for future OPSEC planning. Provisions for feedback must be coordinated with the S2 and the physical security forces to ensure that the requirements to support OPSEC receive the appropriate priority. In addition to intelligence sources providing feedback, OPSEC surveys can provide useful information relating to the success of OPSEC measures.

10. (FOUO) Training. The OPSEC Officer / Coordinator is the manager for all unit OPSEC Training. Newly assigned personnel will receive an OPSEC and security orientation during their in processing. The OPSEC Officer will arrange and conduct general OPSEC awareness training. All personnel will receive an OPSEC refresher as changes in conditions warrant.

11. (U) Plans and Planning.

a. (FOUO) The OPSEC Officer / Coordinator provides planning guidance for development of staff estimates. OPSEC planning guidance is as detailed as time and available information permit. At a minimum it includes the following items:

(1) (FOUO) An estimate of probable adversary knowledge of the activity or operation.

(2) (FOUO) Either specific critical information or categories of critical information to protect.

(3) (FOUO) A preliminary list of CI.

(4) (FOUO) A summary of adversary intelligence collection capabilities.

(5) (FOUO) A list of OPSEC indicators.

(6) (FOUO) A list of OPSEC CM to implement immediately and additional measures to consider.

b. (FOUO) Conduct of Operations. All operations and exercises should incorporate OPSEC CMs that prevent an adversary from detecting or observing friendly actions. This prevents the adversary from delaying, disrupting, or stopping operations. OPSEC CMs apply equally to maneuver forces, combat support, and combat service support operations.

12. (U) Bottom line. How, what, or where we say or type something can seriously endanger friendly personnel, you and your family.

13. (U) This memorandum is in effect until superseded or rescinded.

14. (U) Point of contact for this action is CPT Richard Ward at DSN 847-2229.

2 Encl
1 Critical Information List
2 Counter Measure List

DISTRIBUTION:
Fires Brigade Staff
2-20FA
589th BSB
HHB
A/26FA
324th NSC